JC03 Rec'd PCT/PTO 10 MAY 2001

09/831491

Sughrue
SUGHRUE MION ZINN MACPEAK & SEAS, PLLC

2100 Pennsylvania Avenue, NW
Washington, DC 20037-3213
T 202.293.7060
F 202.293.7860
www.sughrue.com

May 10, 2001

BOX PCT

Commissioner for Patents
Washington, D.C. 20231

PCT/SG98/00088
-filed November 10, 1998

Re: Application of Teow Hin NGAIR
A METHOD OF ENCRYPTION AND APPARATUS THEREFOR
Assignee: KENT RIDGE DIGITAL LABS
Our Ref: Q64409

Dear Sir:

Applicant herewith submit the attached papers for purpose of entering the National Stage under 35 U.S.C. § 371 and in accordance with Chapter II of the Patent Cooperation Treaty: A Preliminary Amendment is attached herewith.

It is assumed that copies of the International Application, the International Search Report, the International Preliminary Examination Report, and any Articles 19 and 34 amendments as required by § 371(c) will be supplied directly by the International Bureau, but if further copies are needed, the undersigned can easily provide them upon request.

Assignment for published patent application is: **KENT RIDGE DIGITAL LABS**.

The Government filing fee is calculated as follows:

Total claims	20	-	20	=		x	$18.00	=	$.00
Independent claims	3	-	3	=		x	$80.00	=	$.00
Base Fee									$1000.00
TOTAL FEE									$1000.00

A check for the statutory filing fee of $1000.00 is attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16, 1.17 and 1.492 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

There is no claim to priority.

Respectfully submitted,

for Alan J. Kasper # 21,092
Registration No. 25,426

SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
+Washington, D.C. 20037-3213
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

Date: May 10, 2001

09/831491
JC03 Rec'd PCT/PTO 10 MAY 2001

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Teow Hin NGAIR

Appln. No.: UNKNOWN

Group Art Unit: UNKNOWN

Confirmation No.: UNKNOWN

Examiner: UNKNOWN

Filed: May 10, 2001

For: A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

PRELIMINARY AMENDMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Prior to examination, please amend the above-identified application as follows:

IN THE CLAIMS:

Please enter the following amended claims:

4. (Amended) A method as claimed in claim 1 further comprising the step of generating a session key for each symmetric key operation.

6. (Amended) A method as claimed in claim 4 wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature.

7. (Amended) A method as claimed in claim 4 further comprising the steps of:

(i) processing the output data to generate a further input related to the output data;

(ii) applying steps (a) and (b) to the further input to create a session bound output;

(iii) combining the session bound output with the token bound output.

8. (Amended) A method as claimed in claim 1 wherein the user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the

token signatures being all combined with the user data or representation to generate the token bound output data.

9. (Amended) A method as claimed in claim 1 wherein the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

10. (Amended) A method of verifying token bound output data created by the method claim 1 by regenerating the token signature using the key employed to encrypt the data and matching it with that in the token bound output.

16. (Amended) Apparatus for performing the method of claim 1.

17. (Amended) Apparatus for performing the method of claim 10.

20. (Amended) A token as claimed in claim 18 being a smartcard.

REMARKS

Entry and consideration of this Amendment is respectfully requested.

Respectfully submitted,

for Alan J. Kasper
Registration No. 25,426

SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
2100 Pennsylvania Avenue, N.W.
Washington, D.C. 20037-3213
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

Date: May 10, 2001

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS:

The claims are amended as follows:

4. (Amended) A method as claimed in ~~any one of claims 1 to 3~~ claim 1 further comprising the step of generating a session key for each symmetric key operation.

6. (Amended) A method as claimed in claim 4 ~~or 5~~ wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature.

7. (Amended) A method as claimed in ~~any one of claims 4 to 6~~ claim 4 further comprising the steps of:

(i) processing the output data to generate a further input related to the output data;

(ii) applying steps (a) and (b) to the further input to create a session bound output;

(iii) combining the session bound output with the token bound output.

8. (Amended) A method as claimed in ~~any one of the preceding claims~~ claim 1 wherein the user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the token signatures being all combined with the user data or representation to generate the token bound output data.

9. (Amended) A method as claimed in ~~any one of the proceeding claims~~ claim 1 wherein the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

10. (Amended) A method of verifying token bound output data created by the method ~~of any one of the preceding claims~~ claim 1 by regenerating the token signature using the key employed to encrypt the data and matching it with that in the token bound output.

16. (Amended) Apparatus for performing the method of ~~any one of claims 1 to 9 or 12~~ claim 1.

17. (Amended) Apparatus for performing the method of ~~any one of claims 10, 11, 13 or 14~~ claim 10.

20. (Amended) A token as claimed in claim 18 ~~or claim 19~~ being a smartcard.

1pd

09/831491
PCT/SG98/00088
Rec'd PCT/PTO 10 MAY 2001

A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

BACKGROUND AND FIELD OF THE INVENTION

This invention relates to a method of encryption and apparatus therefor, particularly for use with a token such as a smart card.

Smart cards, which contain onboard memory and computer processing ability are known. One application for such smart cards is for use as tokens for electronic transactions particularly in the banking sector. The card is used to "sign" a transaction digitally so that the instructed party (a bank in a funds transfer operation, for example) knows that the transaction is instructed by the holder of the card.

Such a transaction begins with the holder inserting the card into a suitable reader connected to a computer terminal in communication with the bank via a telephone line or the internet. The use of a PIN number known only to the holder grants initial access by the holder to the functions provided by the bank to the card holder. The holder can then instruct a transaction and the transaction is authenticated by a public/private key operation using the card. The card provides this by holding a private key of the holder and digitally signing the data. Subsequent verification by the bank using the holder's public key will identify that the

digitally signed instruction came from the holder's card unambiguously.

A disadvantage of transactions such as this is that current smart cards only have limited onboard processing power and since a private key operation requires high computational power, it is not feasible to provide the private key operation for the transaction in the card itself. Instead, this is performed by the terminal to which the card reader is connected. This requires that the private key be provided by the card to the terminal so that the operation may be performed. Once the private key has left the card, however, the security provided by the card will be at risk since the private key may be intercepted or copied. Once this has occurred, it is possible for the holder to be impersonated, since the private key relied upon for authentication of the transaction has been compromised.

It is an object of the invention to alleviate this disadvantage of the prior art.

SUMMARY OF THE INVENTION

According to the invention in a first aspect, there is provided a method of encryption for creating token bound output data from user data using a symmetric key capable token, said method comprising the steps of

a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,

b. retrieving the output of the symmetric key operation as a token signature;and

c. combining the token signature with the user data or representation to generate the token bound output data.

Preferably said representation is a fingerprint of the user data, most preferably generated using a hash function

The method may further comprise the step of generating a session key for each symmetric key operation and the session key may be generated by modifying a symmetric key stored in the token number with a random number.

If a session key is employed, steps (a) and (b) may be conducted recursively and the respective token signatures combined as a single combined token signature and/or the method may further comprise the steps of:

(i) processing the output data to generate a further input related to the output data;

(ii) applying steps (a) and (b) to the further input to create a session bound output;

(iii) combining the session bound output with the token bound output.

The user data or representation may also be split into a

plurality of blocks and separate token signatures are generated for each block, the token signatures being all combined with the user data or representation to generate the token bound output data.

Preferably the output data is used as an input parameter to a private/public key signature generation operation, to form a private/public key signature for the user data.

The invention further provides a method of verifying token bound output data created by the above method by re-generating the token signature using the symmetric key to verify the token, the symmetric key preferably being held by a secure access module at a remote location.

According to the invention in a second aspect, there is provided a method of generating a private key signature in respect of user data using a token, the token having stored therein a private key and a symmetric key, the method comprising the steps of:

a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token;

b. retrieving the output of the symmetric key operation as a token signature;

c. combining the token signature with the user data to generate token bound output data; and

d. providing the output data as an input parameter to a

private key signature generation operation, to form a private key signature for the user data.

The method of the second aspect may further comprise the steps of using a signature verification operation to verify the token bound output data and re-generating the token signature using the symmetric key to verify the token.

The invention extends to apparatus for performing the above methods.

According to the invention in a third aspect, there is provided a token for an electronic transaction, the token supporting a symmetric key operation to generate a token signature from input data. Preferably, the token further stores a private key for a digital transaction signature operation and is embodied as a smartcard.

In the described embodiment, on-line symmetric key authentication of the smart card by a Secure Access Module is employed on top of a private/public key system. The former binds the transaction to the physical smart card that the user is holding. Thus, a two-layer security system is provided in which basic transaction-related operations are protected by the private/public key system and the symmetric key encryption binds these operations with the user's smart card. Hence, as long as at least one of these two security

schemes is not compromised, the resulting signature operation remains secure.

BRIEF DESCRIPTION OF THE DRAWING

An embodiment of the invention will now be described, by way of example, with reference to accompanying Figure 1 which is a schematic diagram of the main structural elements involved in an electronic transaction using the embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

In the following detailed description, reference is made to a specific application of the invention using a Gemplus MPCOS (Multi Payment Card Operating System) smartcard and to use of existing features of this card to provide enhanced cryptographic security. It will be appreciated, however, that the invention is equally applicable for use with other smartcards and tokens generally.

With reference to Figure 1, a Gemplus MPCOS smartcard 10 is shown. The smartcard includes an onboard processor and memory chip 20 connected to data input/output terminals 30. The smartcard 10 is insertable in a reader 40 which includes contacts (not shown) which engage the terminals 30 thus allowing the card to communicate through the reader 40.

The reader 40 is connected to a computer terminal 50 which is in turn connectable via a direct dial-in connection or via the internet to an entity to be instructed, for example an on-line computer 60 at a bank.

The bank's computer 60 is further connectable to a Secure Access Module (SAM) 70 which stores at least one symmetric key also held by the card 10 as described hereinafter. The SAM 70 may be present in the Bank itself or may be held by a trusted third party.

The smartcard 10 of the embodiment of the invention stores not only a private key for electronic transaction use but also a symmetric key such as a triple DES key, for a symmetric encryption operation. The symmetric key is used is the embodiment of the invention to encrypt transaction dependent information which then forms part of the public/private key operation described with reference to the prior art. Since symmetric encryption requires relatively less computational power, this encryption can be conducted by the card processor, so that the symmetric key need never leave the card and thus its security is not compromised.

Using this technique, cryptographic binding of the smartcard to the private key stored therein can be achieved by injecting a smartcard "signature" into the transaction, based on the symmetric key held by the card.

One method of creating such a smartcard signature for a MPCOS Smartcard is via the SELFK command using a card specific key K. More information on this secure messaging command may be found in the Gemplus "MPCOS-3DES Reference Manual".

A generic smartcard signature generation operation using SELFK command has the following steps:

1. The terminal software generates a 8-byte number R, which is essentially random, such as a hash value of user data.

2. The terminal sends the command SELFK(R, Kindex) to the MPCOS card to generate a card signature, where Kindex indicates the secret symmetric key K held by the card to be used for encryption (the card may have several keys, each having a different Kindex).

3. Upon receipt of the instruction, the MPCOS card generates a 8-byte random number CR. The MPCOS card then computes a session key: TK = 3DES(CR, K), by applying a triple DES operation to CR using K. and generates an encrypted output signature: S = 3DES(R, TK), by applying a triple DES operation to R using session key TK.

4. The terminal retrieves both the smartcard signature S and card random number CR.

To verify the signature S based on R and CR, the bank sends these values together with the card serial number (CSN) and Kindex to the SAM 70 which securely holds the symmetric keys associated with the card to re-compute the value of S. If the two S values do match, the bank can be sure that the MPCOS card with the CSN serial number is indeed present. To prevent misuse, the comparison of the S values should only be done in the SAM 70 itself. The comparison result is then output to the bank computer 60.

To achieve this verification, the SAM 70 needs to store the card specific key K. Since many keys for different cards 10 will need to be stored, the SAM 70 may hold a master key, from which all the specific keys K can be derived. The SAM 70, however, needs to be held in a secure environment, for example in the data centre of the bank or other secure premises and guarded with a sound and secure policy.

In actual implementation, the MPCOS card only outputs the 4 least significant bytes of S as a security measure. Therefore, only the 4 least significant bytes are sent by terminal 40 and compared by the SAM 70. However, 4 bytes of signature S may not provide sufficient security strength to prevent an exhaustive search attack. The signature algorithm is preferably, therefore, extended as follows:

1. The terminal software generates the number R.

2. Loop for j from 1 to n, do 2a-2f.

2a. The terminal sends the command SELFK(R, Kindex) to the MPCOS card.

2b. The MPCOS card generates a 8-byte random number CR

2c. The MPCOS card computes TK = 3DES(CR, K), and output S = 3DES(R, TK).

2d. The terminal retrieves both the 4 byte output value S and 8-byte card random number CR.

2e. The terminal concatenates S to an initially empty buffer S′, and similarly concatenates CR to an initially empty buffer CR′.

2f. Loop back to 2a with R now set to a hash function-derived value H(R||S||CR), where || represents concatenation.

Using the above algorithm, cryptogram S′ can have any length, depending upon the number of iterations n and can be used as the MPCOS card signature of the input value R. The signature S' is notionally divided into n four byte elements and corresponding n eight byte elements of random number CR'.

To provide the required verification, the SAM 70 then repeats the algorithm noted using the initial input R, the elements of CR' and the hash function H to generate and verify the elements of S'. For commercial grade security, S′ should preferably have a length of at least 128-bits. This can be achieved by setting the loop number n in step 2 to 4.

For the hash function H used in step 2f above, the implementation may make use of the latest advancements in hash function technology. In particular, use could be made of the HMAC algorithm (Internet RFC 2085, 2104 and 2202) or the simultaneous use of both MD5 and SHA in a secure socket layer protocol (SSL v3).

For convenience the smart card signature (S, CR) or (S′, CR′) generated by the smart card using the above method will hereinafter be referred to as S(R) where R is the input value.

The smartcard signature is applied to a transaction as follows:

In an electronic transaction operation, a digital transaction signature operation is required to verify the user requesting the transaction. The digital transaction signature usually consists of applying a private key operation p to the hash value $h(D)$ of a document D, which is the value R referred to above, such a signature being denoted by $p(h(D))$. To make sure that p is applied with the appropriate smart card, the transaction signature is modified to $p(h(D||S(h(D))))$ or $p(h(D||S'(h(D))))$. Therefore, instead of applying the private key operation to the document directly, this is applied to the hash function fingerprint of the concatenation of the document and the smart card signature of the document.

As in the prior art, the smartcard does not have sufficient computing power to perform the private key operation. Therefore, the private key is output from the card to the terminal 50 which computes the private key operation which generates the digital transaction signature before sending this to the bank computer 60 together with the document, the token signature, the card serial number (CSN) and Kindex.

The bank computer 60 then performs a public key operation using the document transaction signature, the user's public key, the smartcard signature and the document, to verify the document transaction signature. The bank then generates the hash function fingerprint h(D) of the document. The smartcard signature S(R) , card serial number CSN and the hash function fingerprint h(D) are then sent to the SAM 70 which performs the symmetric encryption operation on h(D) using the symmetric key it holds and CR (CR') from the card signature and compares the result with S (S') from the card signature to determine if the signature came from the card identified by the card serial number. If so, an indication is given to the bank computer 60 thus providing a verification that the transaction was conducted with the physical presence of the card 10.

Usually, the length of *h(D)* is longer than the 8-byte number R needed for generating the smart card signature. To use the

whole of h(D) and increase the security strength of the smart card signature further, *h(D)* can be split into 8-byte blocks of $h(D)_1,\ldots,h(D)_m$ (discarding any incomplete trailing block) with each block being processed independently. These processed blocks are then concatenated so that the transaction signature is modified to $p(h(D||S(h(D)_1)||\ldots||S(h(D)_m)))$.

Each block can be processed to form a concatenated signature S' as discussed above. The loop count 2a-2f above for each *S'* can be correspondingly reduced to balance between security and data length.

To verify the digital signature generated with the above it is necessary to transmit the additional values of S and CR (or S′ and CR′) for each element $S(h(D)_1)$-$S(h(D)_m)$ of the smart card signature generated. The verification application of the bank computer 60 will then check the value of each $S(h(D)_i)$ (i = 1 to m) against each pair of $h(D)_i$ and *CR* using the SAM 70 for computation of each S value.

One potential weakness to the above method is that even though a security mechanism is included to ensure that the digital signature is generated with a prior access to the appropriate smartcard, it is not possible for the bank to tell that the smartcard signature is generated during the same *session* as the digital transaction signature. For

example, whenever the smartcard is inserted into a compromised computer, an attacker could possibly generate many smart card signatures with different documents and store them. At a later point when the attacker discovers the user's private key, the correct digital transaction signatures can then be generated without accessing the smart card.

A variation of the method using the following steps can prevent such an attack, by providing a means for the smartcard to encrypt an input related to the signature with the card's session key:

1. Create a file in the Smartcard memory.
2. Create a PIN number to protect access to the file
3. Set the file update permission to allow any application to write to the file in plain text.
4. Set the file read permission to allow MPCOS secure messaging [i.e. encrypted messaging] only.

With such a smart card file, a cryptogram can be generated from the MPCOS card that assures that the digital transaction signature is generated during the same session as the last SELFK command used to create the smartcard signature using the following steps:

1. Do not reset the card after the last SELFK command that

generates the value of $S(h(D))$

2. After the p signing operation, generate a hash m of the digital transaction signature.

3. Present the PIN to unlock the smart card file.

4. Write m into the smart card file using the MPCOS UPDBIN (update binary file) command without secure messaging.

5. Read back the value of m using the MPCOS RDBIN (read binary file) command with secure messaging, that is encrypting m using the session key TK.

The value read in step 5 is added to the digital transaction signature. The SAM 70 then checks encrypted value m as part of the smartcard signature verification routine. With this enhancement, a positive verification by the SAM 70 securely indicates that the public key signature is indeed generated during one single smart card session.

The embodiment described is not to be construed as limitative. For example, the invention is applicable to other kinds of tokens other than smartcards such as a PCMC1A token. The token signature generating method can be used on its own or with other encryption or digital signing techniques, not limited to public/private key operations for digital transaction signature generation as described.

CLAIMS

1. A method of encryption for creating token bound output data from user data using a symmetric key capable token, said method comprising the steps of

a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token,

b. retrieving the output of the symmetric key operation as the token signature; and

c. combining the token signature with the user data or representation to generate the token bound output data.

2. A method as claimed in claim 1 wherein said representation is a fingerprint of the user data.

3. A method as claimed in claim 2 wherein the representation is generated using a hash function

4. A method as claimed in any one of claims 1 to 3 further comprising the step of generating a session key for each symmetric key operation.

5. A method as claimed in claim 4 wherein the session key is generated by modifying a symmetric key stored in the token with a random number.

6. A method as claimed in claim 4 or 5 wherein steps (a) and (b) are conducted recursively and the respective token signatures combined as a single combined token signature.

7. A method as claimed in any one of claims 4 to 6 further comprising the steps of:

(i) processing the output data to generate a further input related to the output data;

(ii) applying steps (a) and (b) to the further input to create a session bound output;

(iii) combining the session bound output with the token bound output.

8. A method as claimed in any one of the preceding claims wherein the user data or representation is split into a plurality of blocks and separate token signatures are generated for each block, the token signatures being all combined with the user data or representation to generate the token bound output data.

9. A method as claimed in any one of the proceeding claims wherein the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

10. A method of verifying token bound output data created by the method of any one of the preceding claims by re-generating the token signature using the key employed to encrypt the data and matching it with that in the token bound output.

11. A method as claimed in claim 10 wherein the symmetric key is held by a secure access module at a remote location.

12. A method of generating a private key signature in respect of user data using a token, the token having stored therein a private key and a symmetric key, the method comprising the steps of:

a. providing the user data or a representation thereof as an input to a symmetric key operation supported by the token;

b. retrieving the output of the symmetric key operation as a token signature;

c. combining the token signature with the user data to generate token bound output data; and

d. providing the output data as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

13. A method of verifying a private key signature generated by the method of claim 12 comprising the steps of using a signature verification operation to verify the token bound

output data and re-generating the token signature using the symmetric key to verify the token.

14. A method as claimed in claim 13 wherein the token signature is verified at a secure location at which the symmetric key is stored.

15. A method as claimed in claim 14 wherein the location is a secure access module.

16. Apparatus for performing the method of any one of claims 1 to 9 or 12.

17. Apparatus for performing the method of any one of claims 10, 11, 13 or 14.

18. A token for an electronic transaction, the token supporting a symmetric key operation to generate a token signature from input data.

19. A token as claimed in claim 18 wherein the token further stores a private key for a digital transaction signature operation.

20. A token as claimed in claim 18 or claim 19 being a smartcard.

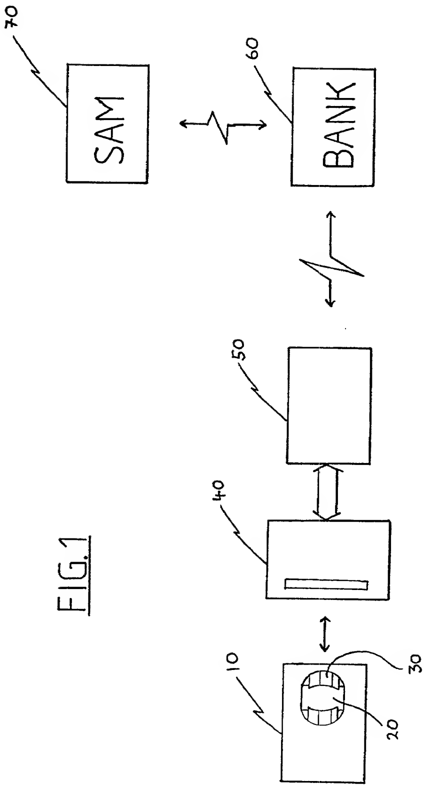

FIG. 1

SOLE/JOIN
Q644(

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that my residence, mailing address and citizenship are as stated below next to my nam that I verily believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (plural names are listed below) of the subject matter claimed and for which a patent is sought in the application entitled:

A METHOD OF ENCRYPTION AND APPARATUS THEREFOR

which application is:
☐ the attached application
(for original application)

PCT Application No. PCT/SG98/00088
☑ Application No. 09/831,491
(Confirmation No.) filed Nov. 10, 1988,
and amended on
(for declaration not accompanying application)

that I have reviewed and understand the contents of the specification of the above-identified application, including the claims, a amended by any amendment referred to above; that I acknowledge my duty to disclose information of which I am aware and which material to the patentability of this application as defined in 37 C.F.R. 1.56, that I hereby claim priority benefits under Title 35, Unite States Code §119(a)-(d) or §365(b) of any foreign application(s) for patent or inventor's certificate, §119(e) of any United State provisional application(s), or §365(a) of any PCT International application which designated at least one country other than the Unite States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or of an PCT International application having a filing date before that of the application on which priority is claimed:

Application Number	Country	Filing Date	Priority Claimed Yes	No

I hereby claim the benefit under 35 United States Code §120 of any United States application(s), or §365(c) of any PCT Internation application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is no disclosed in a listed prior United States or PCT International application in the manner provided by the first paragraph of Title 3. United States Code, §112, I acknowledge my duty to disclose any information material to the patentability of this application a defined in 37 C.F.R. 1.56 which occurred between the filing date of the prior application and the national or PCT international filin date of this application:

Application No.	Filing Date	Status

I hereby appoint John H. Mion, Reg. No. 18,879; Thomas J. Macpeak, Reg. No. 19,292; Robert J. Seas, Jr., Reg. No. 21,092; Darr Mexic, Reg. No. ~~23,063~~; Robert V. Sloan, Reg. No. 22,775; Peter D. Olexy, Reg. No. 24,513; J. Frank Osha, Reg. No. 24,62 Waddell A. Biggart, Reg. No. 24,861; Louis Gubinsky, Reg. No. ~~24,835~~; Neil B. Siegel, Reg. No. ~~25,200~~; David J. Cushing, Reg. N ~~28,703~~; ~~John R.~~ Inge, Reg. No. 26,916; Joseph J. Ruch, Jr., Reg. No. ~~26,577~~; Sheldon I. Landsman, Reg. No. 25,430; Richard C Turner, Reg. No. 29,710; Howard L. Bernstein, Reg. No. 25,665; Alan J. Kasper, Reg. No. 25,426; Kenneth J. Burchfiel, Reg. N ~~31,333~~; Gordon Kit, Reg. No. 30,764; Susan J. Mack, Reg. No. 30,951; Frank L. Bernstein, Reg. No. 31,484; Mark Boland, Reg. N 32,197; William H. Mandir, Reg. No. 32,156; Brian W. Hannon, Reg. No. 32,778; Abraham J. Rosner, Reg. No. ~~33,276~~; Bruce I Kramer, Reg. No. ~~33,725~~; Paul F. Neils, Reg. No. 33,102; Brett S. Sylvester, Reg. ~~No. 32,765~~; Robert M. Masters, Reg. No. 35,60 George F. Lehnigk, Reg. No. 36,359, John T. Callahan, Reg. No. 32,607, Steven M. Gruskin, Reg. No. 36,818, Peter A. McKenn Reg. No. 38,551 and Edward F. Kenehan, Reg. No. 28,962, my attorneys to prosecute this application and to transact all business i the Patent and Trademark Office connected therewith, and request that all correspondence about the application be addressed t **SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC**, 2100 Pennsylvania Avenue, N.W., Washington, D.C. 20037-3213.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and beli are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like s made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willfu false statements may jeopardize the validity of the application or any patent issuing thereon.

Date 19 June 2001 First Inventor Teow Hin NGAIR
First Name Middle Initial Last Name

Residence 334 Kang Ching Road #13-254 Singapore 610334 Signature
City State/Country

SGX

Mailing Address: 334 Kang Ching Road #13-254
Singapore 610334

Citizenship Singapore